WEST Search History

Hide Items | Restore | Clear | Cancel

DATE: Tuesday, August 05, 2008

Hide?	Set Name	Query	Hit Count
	DB=USPT; PLUR=YES; OP=ADJ		
☐	L32	L28 and (first hash value)	0
☐	L31	L28 and multiplexer	0
☐	L30	L28 and multiplexer$.clm.	0
☐	L29	L28 and multiplexer.clm.	0
☐	L28	L25 and (trusted).clm.	1
☐	L27	L25 and (trusted hardware).clm.	0
☐	L26	L25 and hash.clm.	1
☐	L25	L24	1
	DB=PGPB,USPT,USOC; PLUR=YES; OP=ADJ		
☐	L24	L19 and trusted.clm.	3
☐	L23	L20 and (virtual machine monitor).clm.	2
☐	L22	L20 and VMM.clm.	1
☐	L21	L20 and ((virtual machine) near monitor$).clm.	2
☐	L20	((store or storing) same (hash value)).clm.	639
☐	L19	L18	3
	DB=PGPB,USPT,USOC,EPAB,JPAB,DWPI,TDBD; PLUR=YES; OP=ADJ		
☐	L18	L17 and hash.clm.	3
☐	L17	L16 or L15	39
☐	L16	((load or loading) same (VMM)).clm.	22
☐	L15	((load or loading) same ((virtual machine) near monitor$)).clm.	31
☐	L14	((load or loading) and ((virtual machine) near monitor$)).clm.	72
☐	L13	((load or loading) and((virtual machine) near monitor$)).clm.	72
☐	L12	L11 and L10	68

☐	L11	(virtual machine or VM) and trust$	2950
☐	L10	L9 and hash value	109
☐	L9	L8 and hash$	377
☐	L8	L7 or VMM	2226
☐	L7	(virtual machine) near monitor$	1328
☐	L6	L5 and (trust$ or hash$)	3
☐	L5	L4 and ((virtual machine) near monitor$)	11
☐	L4	(L3 or L2)	4300
☐	L3	717/120-123,126-127.ccls.	2348
☐	L2	(717/120 |717/121 |717/127 |717/174 |717/175 |717/176 |717/177 | 717/178).ccls.	3747
☐	L1	20050210467	2

END OF SEARCH HISTORY

L26: Entry 1 of 1 File: USPT May 22, 2007

US-PAT-NO: 7222062
DOCUMENT-IDENTIFIER: US 7222062 B2
**** See image for Certificate of Correction ****

TITLE: Method and system to support a trusted set of operational environments using emulated trusted hardware

DATE-ISSUED: May 22, 2007

PRIOR-PUBLICATION:

DOC-ID	DATE
US 20050138370 A1	June 23, 2005

INVENTOR-INFORMATION:

NAME	CITY	STATE	ZIP CODE	COUNTRY
Goud; Gundrala D.	Olympia	WA		US
Zimmer; Vincent J.	Federal Way	WA		US

US-CL-CURRENT: 703/23; 380/282, 463/29, 711/100, 713/189, 713/193

CLAIMS:

What is claimed is:

1. A method for implementing **trusted** operations within a

computing system using an emulated **trusted** platform module (TPM), comprising: **loading a virtual machine monitor (VMM)** to support a virtual machine (VM) session; **loading** the VM session; **loading** an operating system (OS) into the VM session; and emulating a **trusted** platform module (TPM) to hold a key associated with the VM session and to execute **trusted** operations; determining whether the OS is trustworthy using the key held within the emulated TPM; and terminating the VM sessions along with the OS, if the OS is determined to be untrustworthy.

2. The method of claim 1 wherein emulating the TPM comprises emulating the TPM under the control of the VMM, the VMM to prevent unauthorized access to the key held within the emulated TPM.

3. The method of claim 2 wherein the VMM comprises a layer of software executing below the VM session and having a higher privileged access to system resources than the OS.

4. The method of claim 3 wherein TPM commands originating from within the VM session to execute the **trusted** operations are trapped and redirected to the emulated TPM.

5. The method of claim 1 wherein determining whether the OS is trustworthy comprises determining whether the OS has an unauthorized modification via: hashing at least a portion of the OS to obtain a **hash** value; and comparing the **hash** value to the key held within the emulated TPM.

6. The method of claim 1, further comprising: loading a plurality of VM sessions and a plurality of OS's, each one

of the plurality of OS's loaded into one of the plurality of VM sessions; and emulating a plurality of TPMs each corresponding to one of the plurality of VM sessions, each of the plurality of TPMs to hold a key associated with the corresponding one of the plurality of VM sessions and to execute **trusted** operations.

7. The method of claim 6, further comprising: determining whether each of the plurality of OS's is trustworthy using the key associated with each of the plurality of VM sessions; and terminating any of the plurality of VM sessions supporting an OS determined to be untrustworthy.

8. The method of claim 1 wherein the **trusted** operations include at least one of encrypting data, decrypting data, hashing, and sealing data to a software environment.

9. The method of claim 1, further comprising: denying the OS access to a network domain, if the OS is determined to be untrustworthy.

10. The method of claim 9 wherein denying the OS access to the network domain comprises a management module of a rack of blade servers denying a blade server, executing the OS within the VM session access to the network domain.

11. The method of claim 1 wherein the emulated TPM simulates the functionality of a hardware TPM compliant with a **Trusted** Computing Group's (TCG) **trusted** platform architecture.

12. A machine-readable storage medium that provides instructions that, when executed by a machine, will cause the machine to perform operations for implementing **trusted** operations within a computing system using an emulated **trusted** platform module (TPM), comprising: executing a virtual machine monitor (VMM) to support a virtual machine (VM) session; executing the VM session; executing an operating system (OS) within the VM session; and emulating a **trusted** platform module (TPM) to hold a key associated with the VM session, the VMM to prevent unauthorized access to the key, wherein emulating the TPM further comprises emulating the TPM to allow software applications executing within the OS to establish trust via TPM commands.

13. The machine-readable storage medium of claim 12 wherein the VMM comprises a layer of software executing below the VM session and having a higher privileged access to system resources than the OS.

14. The machine-readable storage medium of claim 12 wherein the TPM commands are trapped and redirected to the emulated TPM.

15. The machine-readable storage medium of claim 12, further providing instructions that, if executed by the machine, will cause the machine to perform operations, comprising: determining whether the OS is trustworthy using the key held within the emulated TPM; and terminating the VM session along with the OS, if the OS is determined to be untrustworthy.

16. The machine-readable storage medium of claim 15 wherein determining whether the OS is trustworthy comprises determining whether the OS has an unauthorized modification

via: hashing at least a portion of the OS to obtain a **hash** value; and comparing the **hash** value to the key.

17. The machine-readable storage medium of claim 12, further providing instructions that, if executed by the machine, will cause the machine to perform operations, comprising: executing the VMM to support a plurality of VM sessions; executing a plurality of VM sessions; executing a plurality of OS's, each one of the plurality of OS's executed within one of the plurality of VM sessions; and emulating a plurality of TPMs each corresponding to one of the plurality of VM sessions, each of the plurality of TPMs to hold a key associated with the corresponding one of the plurality of VM sessions.

18. The machine-readable storage medium of claim 17, further providing instructions that, if executed by the machine will cause the machine to perform operations, comprising: determining whether each of the plurality of OS's is trustworthy using the key associated with each of the plurality of VM sessions; and terminating any of the plurality of VM sessions supporting an OS determined to be untrustworthy.

19. A system for implementing **trusted** operations within a computing system using an emulated **trusted** platform module (TPM), comprising: a processor to execute a **virtual machine monitor (VMM)** to support a virtual machine (VM) session; system memory communicatively coupled to the processor; and a data storage unit (DSU) communicatively coupled to the processor and the system memory and having instructions stored therein to generate the **VMM** and the emulated **trusted** platform module (TPM), the processor coupled to **load the VMM** from the DSU into the system memory, the VM session to support an operating system (OS) therein, the emulated TPM to execute **trusted** operations, wherein the DSU comprises a

firmware unit and the **VMM** comprises a firmware layer to execute below the VM session, the **VMM** having a higher privileged access to the system memory.

20. The system of claim 19 wherein the emulated TPM is further to securely hold a key for executing at least a portion of the **trusted** operations.

21. The system of claim 20 wherein the VMM prevents unauthorized access to the key securely held by the emulated TPM via hiding a memory location of the key.

22. The system of claim 21 wherein the processor is further coupled to execute the VMM and the emulated TPM to determine whether the OS is trustworthy via executing one of the **trusted** operations using the key and to terminate the VM session along with the OS, if the OS is determined to be untrustworthy.

23. The system of claim 19 wherein the emulated TPM emulates the functionality of a TPM compliant with a **Trusted** Computing Group's (TCG) **trusted** platform architecture.

24. A system for implementing **trusted** operations within a server system using an emulated **trusted** platform module (TPM), comprising: a management module; a plurality of blades mounted within a chassis and communicatively coupled to the management module, the plurality of blades each including a data storage unit (DSU) having stored therein instructions to generate the emulated **trusted** platform module (TPM) to hold a key; and a switch communicatively

coupled to the management module and the plurality of blades, the switch to provide the plurality of blades access to a network domain, the switch to deny access of a blade to the network domain, if that one of the plurality of blades is determined to be untrustworthy based on the key.

25. The system of claim 24 wherein the DSU of each of the plurality of blades has further stored therein instructions to generate a virtual machine monitor (VMM) to protect the emulated TPM from unauthorized access and to support a virtual machine (VM) session, the VM session to support an operating system (OS) therein.

26. The system of claim 25 wherein the one of the plurality of blades is determined to be untrustworthy based on the key, if a **hash** of a portion of the OS fails to correspond to the key.

27. The system of claim 25 wherein the key comprises a private key and wherein the one of the plurality of blades is determined to be untrustworthy, if the private key fails to correspond to a public key obtained from a **trusted** third party.

Previous Doc Next Doc Go to Doc#